Doc Code:

PTO/SB/21 (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

Application Number	09/746,015
Filing Date	December 26, 2000
First Named Inventor	LANGFORD, Glenn
Art Unit	2131
Examiner Name	ABRISHAMKAR, Kaveh
Attorney Docket Number	77666-8 /jas

ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
- ☐ Fee Attached
- ☐ Amendment / Reply
- ☐ After Final
- ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
- ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
- ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☒ Other Enclosure(s) (please identify below):

1. Appellant's Brief Under 37 CFR 1.192 in response to the Notice of Non-Compliant Appeal Brief dated October 12, 2006.

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	SMART & BIGGAR		
Signature			
Printed name	R. ALLAN BRETT		
Date	NOVEMBER 3, 2006	Reg. No.	40,476

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria,VA 22313-1450 on the

Signature			
Typed or printed name		Date	

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE HONORABLE BOARD OF PATENT APPEALS

In re application of:	
Glenn Langford	Group Art Unit: 2131
Serial No.: 09/746,015	Examiner: Abrishamkar, Kaveh
Filed: December 26, 2000	Attorney Docket: 77666-8
For: KEY RELEASE SYSTEMS, COMPONENTS AND METHODS	

APPELLANT'S BRIEF UNDER 37 C.F.R. 1.192

The Assistant Commissioner of Patents
Washington, D.C. 20231
U.S.A.

Dear Sir or Madam:

The following is the Appellant's Brief, submitted under the provisions of 37 C.F.R. 1.192. The fee of $500 required by 37 C.F.R. 1.17(c) was paid with our earlier submission filed on September 28, 2006.

Real Party in Interest

The real party in interest is the assignee of record, i.e. Entrust Limited, 1000 Innovation Drive, Ottawa, Ontario, K2K 3E7, Canada.

Related Appeals and Interferences

There are no related appeals or interferences that will directly affect, be directly affected by or have a bearing on the present appeal.

Status of Claims

Claims 1 to 11, 13 to 33 and 35 to 42 are presently pending in this application.

Claim 31 stands rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter. Applicant hereby requests that Claims 31 and 32 be cancelled.

Claims 13 to 30 and 38 to 42 stand rejected under 35 U.S.C. 102(b) as being anticipated by Ford et al. (U.S. Patent 5,481,613). Claims 1 to 11 and 31 to 47 stand rejected under 35 U.S.C. 103 as being unpatentable over Ford

The present appeal is directed to claims 1 to 11, 13 to 30 and 35 to 42.

Status of Amendments

The Appellant filed an amendment to claim 31 in reply to the Final Office Action on May 11, 2006. In an Advisory Action of June 7, 2007, it was stated this amendment would not be entered.

Applicant hereby submits an amendment cancelling claims 31 and 32. The claims, as amended, are enclosed herewith in the Appendix of Claims.

Summary of the Claimed Subject Matter

The invention is embodied in the five appealed independent claims, namely

claims 1, 13, 30, 33 and 38.

Claim 1 is directed to a method for a decryptor 12 to obtain a decryption key from a key release agent 14. The decryptor obtains an encryption block 56, generates a key release request 64 and outputs the key release request 64 to the key release agent 14. The encryption block 12 comprises a data ciphertext 44 requiring a decryption key to decrypt, key related information (page 18 lines 8 to 13) associated with a first {public key, private key} pair, and a key ciphertext consisting of the decryption key encrypted by the first public key. The encryption block 12 does not include an ACD (access controlled decryption) block. The key release request 64 contains the key ciphertext and the key related information. The key release request 64 is for use by the key release agent 14 to locate decryptor authorization logic (page 15 lines 2 to 3) stored externally to the key release request. The logic is to be applied in determining whether or not to release the decryption key. If the decryption key is to be release, the decryptor receives a key release response 66 specifying the decryption key. (See also page 7 line 24 to page 8 line 9 and page 13 line 6 to page 14 line 7).

Claim 13 is directed to a key release method. A key ciphertext and key related information are received from decryptor 12. The key related information is in respect of a key used to encrypt the key ciphertext. Decryptor authorization logic (page 15 lines 2 to 3) stored externally to the decryptor is located with use of the key related information. Decryptor information (page 18 lines 15 to 23) with respect to the decryptor is located. Whether decryption of the key ciphertext is to be permitted is decided. The decision is based on the decryptor information and the decryptor information logic. (See page 5 lines 9 to 16; page 16 line 23 to page 18 line 4).

Claim 30 is directed to a method of controlling access to a decryption key. A key release request 64 is received from a decryptor 12. The request comprises decryptor information (page 18 lines 15 to 23) and the decryption key encrypted using a public key. Decryption authorization logic (page 15 lines 2 to 3) stored externally to the request is located with the use of the public key. The logic is applied to the decryption information

to determine whether the decryptor should be permitted access to the decryption key. If the decryptor is to be permitted access, a key release 66 response specifying the decryption key is sent. (See page 6, lines 25 to page 7 line 19; page 14 lines 8 to 18).

Claim 33 is directed to a decryptor 12 comprising means for obtaining an encryption block 56, means for generating a key release request 64 and outputting the request to a key release agent 14, means for making decryptor information (page 18 lines 15 to 23) available to the key release agent, and means for receiving a key release response 66. The encryption block comprises a data ciphertext requiring a decryption key to decrypt, key related information (page 18 lines 8 to 13) associated with a first {public key, private key} pair and a key ciphertext consisting of the decryption key encrypted by the first public key/ The encryption block does not include an ACD. The key release request contains the key ciphertext and the key related information. The decryptor information is for use by the key release agent to locate decryptor authorization logic (page 15 lines 2 to 3) stored externally to the key release request. The logic is to be applied in determining whether or not to release the decryption key. (See page 7 lines 20 to 23 and page 12 lines 28 to page 13 line 15).

Claim 38 is directed to a key release agent 14 comprising means for receiving from a decryptor 12 a key cipher text and key related information (page 18 lines 8 to 13) in respect of a key used to encrypt the key ciphertext, means for locating decryptor information (page 18 lines 15 to 23) stored externally to the decryptor with use of the key related information, means for locating decryptor information in respect of the decryptor, and means for deciding based on decryptor information and the decryptor authorization logic (page 15 lines 2 to 3) whether decryption of the ciphertext is to be permitted. (Page 14 line 8 to 18; page 15 lines 21 to 25).

Grounds of Rejection to be Reviewed on Appeal

Claims 13 to 30 and 38 to 42 are rejected under 35 U.S.C. 102(b) as being anticipated by Ford et al. (U.S. Patent 5,481,613) (hereinafter "Ford").

Claims 1 to 11 and 31 to 47 are rejected under 35 U.S.C. 103 as being unpatentable over Ford.

Argument

35 U.S.C. 102(b)

1. Independent Method Claim 13

It is respectfully submitted that the Examiner's rejection of claim 13 is erroneous, for the following reasons.

The Examiner alleges that the feature of "locating decryptor authorization logic stored externally to the decryptor with use of the key related information" is disclosed in Ford in Figure 2 and at column 6, lines 13 to 17 and 53 to 55 and that the feature of "obtaining decryptor information in respect of the decryptor" is disclosed in Ford at column 6, lines 56–66. The referenced passages of Ford refer to obtaining "decryptor privilege attribute information" and provide examples of what that information can include. These include: authenticated identity, group membership, role membership, and clearance information. The Examiner has inferred that the decryptor privilege attribute information of Ford is analogous to both the decryptor authorization logic and the decryptor information recited in claim 13. Lines 55-66 simply provide examples of the decryption privilege attribute information disclosed on lines 50-55. Therefore, both passages are referring to the same thing. With all due respect, this interpretation of the claims and prior art results in the illogical result of the decryptor authorization logic and the decryptor information having the same meaning. This is clearly an error.

The terms "logic" and "information" have been used by the Applicant throughout the claims and description in different contexts and it is clear that these terms are intended to have different meanings. For example, the limitation of "deciding based on

the decryptor information and the decryptor authorization logic ..." in claim 13 would be nonsensical if these two terms did not have different meanings. In any event, the ordinary meaning of these terms, as understood by a person skilled in the art are clearly different. Information does not have any functionality, whereas logic can be applied to information or data to achieve a result.

As explained on page 13 of our response of December 13, 2005, the decryptor privilege attribute information is clearly not "decryptor logic". The following passage from Ford referred to on that page of the response, makes it clear that the decryptor attribute information is simply data that is used as the basis for a comparison:

> "This decryptor privilege attribute information may be just the decryptor's authenticated identity, which may be obtained in one embodiment through the key release transaction request using a suitable authentication mechanism. In another embodiment, more extensive decryptor privilege attribute information, e.g., group-membership, role-membership, or clearance information may be supplied by the decryptor in a certified form, e.g., a privilege attribute certificate signed by a trusted third party, or, in a yet further embodiment, the KRA may obtain decryptor privilege attributes from a supporting database as shown by a dotted line in FIG. 2. "

It is clearly wrong to interpret "decryptor privilege attribute information" to be analogous to "logic" that can be applied to data, as the Examiner has done in the Advisory Action. On page 15 of the description of the present invention, in describing a specific embodiment, it is stated on lines 1-4 that: "Each access identifier is associated with a set of rules (more generally, is associated with respective decryptor authorization logic)". Clearly, a set of rules is an example of logic. However, the "decryptor privilege attribute information", as used in the context of Ford could not be used to describe a set of rules.

Therefore, the essential feature of "locating decryptor authorization logic stored

externally to the decryptor" in claim 13 is not disclosed by the prior art and thus the test for anticipation has not been met. It is thus respectfully submitted that claim 13 is in compliance with 35 U.S.C. 102(b).

2. Dependent Claim 14

Claim 14 depends from claim 13 and defines the additional limitation of the decryptor information being received from the decryptor together with the key ciphertext and key related information.

Claim 14 includes the inventive features of claim 13 and therefore, it is respectfully submitted that claim 14 is novel over Ford for at least the reasons given with respect to claim 13.

Furthermore, it is submitted that the additional limitation recited in claim 14 is not disclosed in the cited passage of Ford, i.e. Figure 2, step 34, column 6, line 40 to column 7, line 49. The cited passage does not disclose obtaining the decryptor information from the decryptor nor receiving it together with key ciphertext and key related information. At lines 42 to 43 of column 6, Ford states that: "The KRA will also obtain decryptor privilege information". This leads the reader to understand that the decryptor privilege information is obtained in addition to the other information but not at the same time or from the same place. In fact, in the specific embodiment shown in Figure 2, the decryptor privilege information is obtained from a supporting database.

Therefore, it is respectfully submitted that claim 14 is in compliance with 35 U.S.C. 102(b).

3. Dependent Claim 15

Claim 15 depends from claim 13 and defines the additional limitation of receiving the decryptor information while establishing a secure connection with the decryptor.

Claim 15 includes the inventive features of claim 13 and therefore, it is respectfully submitted that claim 15 is novel over Ford for at least the reasons given with respect to claim 13.

In addition, it is submitted that the additional limitations recited in claim 15 are not disclosed in the cited passage of Ford, i.e. Figure 2, step 34, column 6, line 40 to column 7, line 49. As stated with respect to claim 14, the cited passage of Ford does not disclose obtaining the decryptor information from the decryptor. Furthermore, there is no disclosure in the cited passage of establishing a secure connection with the decryptor while obtaining the decryptor information.

Therefore, it is respectfully submitted that claim 15 is in compliance with 35 U.S.C. 102(b).

4. Dependent Claim 16

Claim 16 depends from claim 13 and defines the additional limitations of receiving from the decryptor a decryptor identifier and using the decryptor identifier to lookup decryptor attibutes from a public repository, the decryptor identifier and decryptor attributes together constituting the decryptor information.

Claim 16 includes the inventive features of claim 13 and therefore, it is respectfully submitted that claim 16 is novel over Ford for at least the reasons given with respect to claim 13.

In addition, it is submitted that the additional limitations recited in claim 16 are not disclosed in the cited passage of Ford, i.e. Figure 2, step 34, column 6, line 40 to

column 7, line 49. As stated with respect to claim 14, the cited passage of Ford does not disclose obtaining the decryptor information from the decryptor. As well, the cited passage of Ford does not disclose using a decryptor identifier to lookup decryptor attributes. What is disclosed in column 6, lines 42 to 65 of Ford is that decryptor privilege attribute information can include the decryptor's authentication identity and that the attributes may be obtained from a supporting database. The use of an identifier to lookup other attributes is not disclosed.

Therefore, it is submitted that claim 16 is in compliance with 35 U.S.C. 102(b).

5. Dependent Claim 19

Claim 19 depends from Claim 17 and defines the additional limitation of receiving the certificate together with the key ciphertext and key related information.

Claim 19 includes the inventive features of claim 13 and therefore, it is respectfully submitted that claim 19 is novel over Ford for at least the reasons given with respect to claim 13.

Furthermore, it is submitted that the additional limitations recited in claim 19 are not disclosed in the cited portions of Ford At lines 42 to 43 of column 6, Ford states that: "The KRA will also obtain decryptor privilege information". This leads the reader to understand that the information, which could include a certificate is obtained in addition to the other information but not together with it.

Therefore, it is respectfully submitted that claim 19 is in compliance with 35 U.S.C. 102(b).

6. Dependent Claims 25, 26 and 27

Claim 25 depends from claim 13 and defines the further limitations of receiving a

plurality of key ciphertexts and respective key related information from the decryptor and determining whether at least one private key required to decrypt a respective at least one key ciphertext of the plurality of key ciphertexts is available; using the respective key related information to locate respective decryptor authorization logic stored externally to the decryptor; and upon determining such at least one private key is available, deciding based on the decryptor information and the respective decryptor authorization logic whether decryption of at least one of the plurality of key ciphertexts is permitted.

Claim 25 includes the inventive features of claim 13 and therefore, it is respectfully submitted that claim 25 is novel over Ford for at least the reasons given with respect to claim 13.

Furthermore, it is submitted that the cited passages of Ford do not disclose the additional limitations of claim 25. In particular, column 6 lines 24 to 40 do not discuss the availability of the private key. Because Ford does not disclose decryptor authorization "logic", as discussed with reference to claim 13, it also does not disclose using key related information to locate the logic nor does it disclose deciding based on the logic in combination with decryptor information whether decryption is permitted.

Claims 26 and 27 depend from claim 25 and include the inventive features of claim 25 and therefore are novel over Ford for at least the reasons given with respect to claim 25.

Therefore, it is respectfully submitted that claims 25 to 27 are in compliance with 35 U.S.C. 102(b).

7. Dependent Claim 28

Claim 28 depends from claim 13 and defines the further limitation that deciding based on decryptor information of the decryptor and the decryptor authorization logic whether decryption of the key ciphertext is to be permitted comprises applying at least

one rule of the decryptor authorization logic associated with the public key used to encrypt the decryption key to the decryptor information to determine whether the decryptror should be permitted access to the decryption key.

Claim 28 includes the inventive features of claim 13 and therefore, it is respectfully submitted that claim 28 is novel over Ford for at least the reasons given with respect to claim 13. Furthermore, making a decision based on logic that is not disclosed is necessarily also not disclosed.

Therefore, it is respectfully submitted that claim 28 is in compliance with 35 U.S.C. 102(b).

8. Dependent Claims 17, 18 and 20 to 24

Dependent Claims 17, 18, and 20 to 24 depend either directly or indirectly from claim 13 and thus include the inventive features of claim 13. Therefore, it is respectfully submitted that claims 17, 18, and 20 to 24 are novel over Ford for at least the reasons given with respect to claim 13 and thus are in compliance with 35 U.S.C. 102(b).

9. Independent Claim 29

Independent claim 29 also contains the limitation of "locating decryptor authorization logic stored externally to the decryptor". As explained with respect to independent claim 13, this feature is not disclosed in Ford

Furthermore, claim 29 recites "applying the decryptor authorization logic to encrypt the decryption key to the decryptor information to determine whether the decryptor should be permitted access to the decryption key". The passage of Ford cited by the Examiner as disclosing this feature, namely Figure 2 and column 7, lines 35 to 49, actually discloses the application of Access Control Attributes (ACA) with the decryptor privilege attributes. The ACA is included in the ACD block with the key-release request - not stored externally. Ford does not disclose applying logic retrieved from an external

storage. Therefore, Ford does not disclose all of the essential features of this claim and the test for anticipation has not been met.

Thus, it is respectfully submitted that claim 29 is in compliance with 35 U.S.C. 102(b).

10. Independent Claim 30

Regarding independent claim 30, this claim is hereby cancelled.

11. Independent Claim 38

With respect to independent claim 38, it recites "means for locating decryptor authorization logic stored externally to the decryptor" and "means for deciding based on decryptor information of the decryptor and the decryptor authorization logic". These are means for implementing the method steps of claim 13 and therefore the claim is novel over Ford for at least the same reasons given with respect to that claim. Specifically, Ford does not disclose "decryptor authorization logic stored externally to the decryptor".

Thus, it is respectfully submitted that claim 38 is in compliance with 35 U.S.C. 102(b).

12. Dependent Claim 39

Claim 39 depends from claim 38 and defines the further limitation that the key release agent is adpated to receive the decryptor information with the key ciphertext and key related information.

Claim 39 includes the inventive features of claim 38 and therefore, it is respectfully submitted that claim 39 is novel over Ford for at least the reasons given with respect to claim 38.

Furthermore, it is submitted that the additional limitation recited in claim 39 is not disclosed in the cited passage of Ford, i.e. Figure 2, and column 6, lines 24 to 40. The cited passage does not disclose obtaining the decryptor information from the decryptor nor receiving it together with key ciphertext and key related information.

Therefore, it is respectfully submitted that claim 39 is in compliance with 35 U.S.C. 102(b).

13. Dependent Claim 40

Claim 40 depends from claim 38 and defines the further limitation of the key release agent being adapted to use a decryptor identifier to lookup decryptor attributes from a repository, the decryptor identifier and the decryptor attributes together constituting the decrpyptor information.

Claim 40 includes the inventive features of claim 38 and therefore, it is respectfully submitted that claim 40 is novel over Ford for at least the reasons given with respect to claim 38.

In addition, it is submitted that the additional limitations recited in claim 40 are not disclosed in the cited passage of Ford, i.e. column 6, lines 42 to 65. The cited passage of Ford does not disclose obtaining the decryptor information from the decryptor. As well, the cited passage of Ford does not disclose using a decryptor identifier to lookup decryptor attributes. What is disclosed in column 6, lines 42 to 65 of Ford is that decryptor privilege attribute information can include the decryptor's authentication identity and that the attributes may be obtained from a supporting database. The use of an identifier to lookup other attributes is not disclosed.

Therefore, it is submitted that claim 40 is in compliance with 35 U.S.C. 102(b).

14. Dependent Claim 41

Claim 41 includes the inventive features of claim 38 and therefore, it is respectfully submitted that claim 41 is novel over Ford for at least the reasons given with respect to claim 38 and in compliance with 35 U.S.C. 102(b).

15. Dependent Claim 42

Claim 42 depends from claim 38 and defines the further limitation of a means for applying decryptor authorization logic associated with each public key used to encrypt the decryption key to the decryptor information for determining whether the decryptor should be permitted access to the decryption key.

Claim 42 includes the inventive features of claim 38 and therefore, it is respectfully submitted that claim 42 is novel over Ford for at least the reasons given with respect to claim 38. Furthermore, applying logic that is not disclosed is necessarily also not disclosed.

Therefore, it is respectfully submitted that claim 42 is in compliance with 35 U.S.C. 102(b).

35 U.S.C. 103

16. Independent Claim 1

Claims 1 also includes the feature of decryptor authorization logic stored external to the decryptor and therefore a prima facie case for obviousness has not been met because, all of the claim limitations have not been disclosed in the cited prior art.

In particular, Claim 1 recites "the decryptor generating a key release request ... for use by the key release agent to locate decryptor authorization logic stored externally to the key release that is to be applied". Once again, the passages from Ford cited by the Examiner disclose attribute information and not decryptor authorization logic.

Therefore, it is respectully submitted that a prima facie case for obviousness has not been made out and that claim 1 is in compliance with 35 U.S.C. 103.

17. Dependent Claims 2, 3, 4, 6, 7, 8, 9, 10, 11

Claims 2 to 4 and 6 to 11 include all of the inventive features of claim 1 and therefore are inventive over Ford for at least the reasons given with respect to claim 1. Therefore, it is respectfully submitted that claims 2 to 4 and 6 to 11 are in compliance with 35 U.S.C. 103.

18. Dependent Claim 5

Claim 5 depends from claim 2 and defines the further limitation that the decryptor making the decryptor information available to the key release agent comprises the decryptor providing the decryptor information to the key release agent while establishing a secure connection with the key release agent.

Claim 5 includes all of the inventive features of claim 1 and therefore is inventive over Ford for at least the reasons given with respect to claim 1. Furthermore, as submitted with reference to claim 15, the additional features claimed in claim 5 are not disclosed in Ford. Therefore, a *prima facie* case for obviousness has not been met and it is submitted that claim 5 is in compliance with 35 U.S.C. 103.

19. Independent claim 33

Claim 33 also includes the feature of decryptor authorization logic stored external

to the decryptor and therefore a *prima facie* case for obviousness has not been met because all of the claim limitations have not been disclosed in the cited prior art. Therefore, for at least the reasons given with respect to claim 1, it is respectfully submitted that claim 33 is in compliance with 35 U.S.C. 103.

20. Dependent Claims 35 to 37

Claims 35 to 37 include all of the inventive features of claim 33 and therefore are inventive over Ford for at least the reasons given with respect to claim 33. Thus, it is respectfully submitted that claims 35 to 37 are in compliance with 35 U.S.C. 103.

Summary

For the foregoing reasons, it is submitted that the Examiner's rejections are erroneous, and reversal of his decision is respectfully requested.

Respectfully submitted,

GLENN LANGFORD

By
Allan Brett
Reg. No. 40476
Tel.: (613) 232-2486, Ext. 323

Smart & Biggar
P.O. Box 2999, Station D
900-55 Metcalfe Street
Ottawa, Ontario K1P 5Y6

Date: November 3, 2006

RAB:KLM:mmc

Claims Appendix:

1. (Previously presented) A method for a decryptor to obtain a decryption key from a key release agent comprising:

a decryptor obtaining an encryption block comprising a data ciphertext requiring a decryption key to decrypt, the encryption block further comprising key related information associated with a first {public key, private key} pair, the encryption block further comprising a key ciphertext consisting of the decryption key encrypted by the first public key of the first {public key, private key} pair, the encryption block not including an ACD (access controlled decryption) block;

the decryptor generating a key release request containing the key ciphertext, and the key related information and outputting the key release request to the key release agent, the key release request for use by the key release agent to locate decryptor authorization logic stored externally to the key release request that is to be applied in determining whether or not to release the decryption key;

in the event the decryption key is to be released, the decryptor receiving a key release response specifying the decryption key.

2. (Previously presented) A method according to claim 1 further comprising:

the decryptor making decryptor information available to the key release agent, the decryptor information for use by the key release agent in determining decryptor attributes, the decryptor attributes for further use in determining whether or not to release the decryption key.

3. (Original) A method according to claim 1 further comprising the decryptor using the decryption key to decrypt the data ciphertext.

4. (Original) A method according to claim 1 wherein the decryptor making the decryptor information available to the key release agent comprises including the decryptor information in the key release request.

5. (Previously presented) A method according to claim 2 wherein the decryptor making the decryptor information available to the key release agent comprises the decryptor providing the decryptor information to the key release agent while establishing a secure connection with the key release agent.

6. (Previously presented) A method according to claim 2 wherein the decryptor making the decryptor information available to the key release agent comprises providing a decryptor identifier which may be used to look up decryptor attributes stored in a repository external to the key release request.

7. (Original) A method according to claim 1 wherein the key related information comprises a key pair identifier.

8. (Original) A method according to claim 1 further comprising:

before generating the key release request, the decryptor determining if the private key of the first {public key, private key} pair is available at the decryptor;

upon determining the private key of the first {public key, private key} pair is not available at the decryptor generating the key release request.

9. (Original) A method according to claim 1 further comprising:

decrypting at least a portion of the key release response containing an encrypted version of the decryption key using a private key of a second {public key, private key} pair to recover the decryption key.

10. (Previously presented) A method according to claim 1 wherein the encryption block comprises a plurality of key related information associated with a respective plurality of first {public key, private key} pairs, and a respective plurality of key ciphertexts each consisting of the decryption key encrypted by the public key of a respective one of the plurality of first {public key, private key} pairs associated with the plurality of key related information, the method comprising:

generating the key release request containing the plurality of key

ciphertexts, and the associated plurality of key related information.

11. (Original) A method according to claim 10 further comprising:

before generating the key release request, determining if at least one private key of the plurality of first {public key, private key} pairs is available at the decryptor;

upon determining none of the private keys of the plurality of first {public key, private key} pairs is available at the decryptor generating the key release request.

12. (Cancelled)

13. (Previously presented) A key release method comprising:

receiving a key ciphertext and key related information in respect of a key used to encrypt the key ciphertext from a decryptor;

locating decryptor authorization logic stored externally to the decryptor with use of the key related information;

obtaining decryptor information in respect of the decryptor;

deciding based on the decryptor information and the decryptor authorization logic whether decryption of the key ciphertext is to be permitted.

14. (Original) A method according to claim 13 wherein the decryptor information is received from the decryptor together with the key ciphertext and key related information.

15. (Original) A method according to claim 13 wherein obtaining decryptor information comprises receiving the decryptor information while establishing a secure connection with the decryptor.

16. (Original) A method according to claim 13 wherein obtaining decryptor information comprises:

receiving from the decryptor a decryptor identifier;

using the decryptor identifier to lookup decryptor attributes from a public repository, the decryptor identifier and decryptor attributes together constituting the decryptor information.

17. (Original) A method according to claim 13 further comprising:

using information in a certificate as the decryptor information.

18. (Original) A method according to claim 17 further comprising:

obtaining the certificate from a certificate repository.

19. (Original) A method according to claim 17 further comprising receiving the certificate together with the key ciphertext and key related information.

20. (Original) A method according to claim 13 wherein the decryptor information is an identity or role of the decryptor, an alias, or a claim of access rights or privilege, or some other attribute of the decryptor of a corresponding decrypting device or platform.

21. (Original) A method according to claim 13 wherein the key related information comprises a key pair identifier.

22. (Original) A method according to claim 13 further comprising:

decrypting the key ciphertext, re-encrypting the key using a public key of a {public key, private key} pair to produce a re-encrypted key, the private key of which is available to the decryptor, and sending the re-encrypted key to the decryptor.

23. (Original) A method according to claim 13 further comprising:

decrypting the key ciphertext to obtain a decryption key;

sending the decryption key to the decryptor over a secure channel.

24. (Original) A method according to claim 13 further comprising:

decrypting the key ciphertext to obtain a decryption key;

using a symmetric key available to the decryptor, encrypting the decryption key with the symmetric key to produce an encrypted decryption key, and sending the encrypted decryption key to the decryptor.

25. (Previously presented) A method according to claim 13 further comprising:

receiving a plurality of key ciphertexts and respective key related information from the decryptor and determining whether at least one private key required to decrypt a respective at least one key ciphertext of the plurality of key ciphertexts is available;

using the respective key related information to locate respective decryptor authorization logic stored externally to the decryptor; and

upon determining such at least one private key is available, deciding based on the decryptor information and the respective decryptor authorization logic whether decryption of at least one of the plurality of key ciphertexts is to be permitted.

26. (Original) A method to claim 25 further comprising:

decrypting one of the key ciphertexts using a corresponding private key to recover a decryption key.

27. (Previously presented) A method according to claim 25 wherein deciding based on decryptor information of the decryptor and the respective decryptor authorization logic whether decryption of at least one of the key ciphertexts is to be permitted comprises applying the respective decryptor authorization logic associated with each public key used to encrypt the decryption key to the decryptor information to determine whether the decryptor should be permitted access to the decryption key.

28. (Previously presented) A method according to claim 13 wherein deciding based on decryptor information of the decryptor and the decryptor authorization logic whether decryption of the key ciphertext is to be permitted comprises applying at least one rule of the decryptor authorization logic associated with the public key used to encrypt the decryption key to the decryptor information to determine whether the decryptor should be

permitted access to the decryption key.

29. (Previously presented) A method of controlling access to a decryption key comprising:

receiving from a decryptor a key release request comprising decryptor information and the decryption key encrypted using a public key;

locating decryption authorization logic stored externally to the key release request with use of the public key;

applying the decryption authorization logic to the decryptor information to determine whether the decryptor should be permitted access to the decryption key;

upon determining the decryptor should be permitted access to the decryption key, sending a key release response specifying the decryption key.

30. (Previously presented) A method of controlling access to decryption keys comprising:

maintaining a private key repository comprising a plurality of access identifiers, and for each access identifier at least one key related information of a respective {public key, private key} pair, the repository also containing the private key of each {public key, private key} pair;

receiving a key release request containing a decryption key encrypted using a public key of a {public key, private key} pair and containing a key related information associated with the {public key, private key} pair;

maintaining a repository residing externally to the key release request associating each access identifier with respective decryptor authorization logic that can be applied to a decryptor information;

obtaining decryptor information;

for each access identifier in association with which the key related

information is stored, applying the respective decryptor authorization logic to the decryptor information specified in the key release request;

in the event the decryptor information satisfies at least one of the respective decryptor authorization logics, decrypting the ciphertext to recover the decryption key, and sending a key release response to the decryptor specifying the decryption key.

31. (Cancelled)

32. (Cancelled)

33. (Previously presented) A decryptor comprising:

means for obtaining an encryption block comprising a data ciphertext requiring a decryption key to decrypt, the encryption block further comprising key related information associated with a first {public key, private key} pair, the encryption block further comprising a key ciphertext consisting of the decryption key encrypted by the first public key of the first {public key, private key} pair, the encryption block not including an ACD (access controlled decryption) block;

means for generating a key release request containing the key ciphertext, and the key related information and outputting the key release request to the key release agent;

means for making decryptor information available to the key release agent, the decryptor information for use by the key release agent to obtain decryptor authorization logic stored externally to the key release request that is to be applied in determining whether or not to release the decryption key;

means for receiving a key release response specifying the decryption key.

34. (Cancelled)

35. (Previously presented) A decryptor according to claim 33 further comprising means

for using the decryption key to decrypt the data ciphertext.

36. (Original) A decryptor according to clam 33 adapted to make the decryptor information available to the key release agent by including the decryptor information in the key release request.

37. (Original) A decryptor according to claim 33 further comprising means for decrypting at least a portion of the key release response containing an encrypted version of the decryption key using a private key of a second {public key, private key} pair to recover the decryption key.

38. (Previously presented) A key release agent comprising:

means for receiving from a decryptor a key ciphertext and key related information in respect of a key used to encrypt the key ciphertext;

means for locating decryptor authorization logic stored externally to the decryptor with use of the key related information;

means for obtaining decryptor information in respect of the decryptor; and

means for deciding based on decryptor information of the decryptor and the decryptor authorization logic whether decryption of the key ciphertext is to be permitted.

39. (Original) A key release agent according to claim 38 adapted to receive the decryptor information together with the key ciphertext and key related information.

40. (Previously presented) A key release agent according to claim 38 adapted to use a decryptor identifier to lookup decryptor attributes from a repository, the decryptor identifier and decryptor attributes together constituting the decryptor information.

41. (Previously presented) A key release agent according to claim 38 further comprising:

decrypting means for decrypting the key ciphertext;

encryption means for re-encrypting the key using a public key of a {public key, private key} pair to produce a re-encrypted key, the private key of which is available to the decryptor;

means for sending the re-encrypted key to the decryptor.

42. (Previously presented) A key release agent according to claim 38 further comprising:

means for applying decryptor authorization logic associated with each public key used to encrypt the decryption key to the decryptor information for determining whether the decryptor should be permitted access to the decryption key.

Evidence Appendix:

None.

Related Proceedings Appendix

None